

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO**

---

**UNITED STATES OF AMERICA,**

Plaintiff,

v.

No. CR 10-2626 BB

**PEDRO LEONARDO MASCHERONI,**  
also known as “Luke”, and **MARJORIE**  
**ROXBY MASCHERONI,**

Defendants.

**MEMORANDUM OPINION**

This matter comes before the Court for consideration of Plaintiff’s (“the Government”) motion requesting entry of a protective order. [Doc. 171] The Court has considered the submissions of the parties and the applicable law, and will enter such a protective order in substantially the form proposed by the Government, as discussed below.

**Background**

Defendants have been indicted on a number of charges alleging they communicated classified information and conspired to communicate such information, in connection with a conspiracy to participate in the development of an atomic weapon. The case has been pending since September 16, 2010. At the outset of the case, the Government seized 200 boxes of documents from Defendants, containing 276,000 pages of documents. The Government also seized electronic data totaling 5.8 terabytes. In order to fulfill discovery obligations, the Government wishes to give Defendants access to the documents and other data, but is unwilling to do so in the absence of a protective order intended to prevent the inadvertent or advertent

disclosure of classified information allegedly contained in the materials seized from Defendants. The Government has proposed such a protective order (“P.O.”), to which Defendants strongly object.

Under the P.O. all of the material seized from Defendants would be treated as potentially classified information, requiring Defendants to deal with it as such.<sup>1</sup> Defendants would not be allowed to use the information in pleadings or place it before the public in any other way, until the information has been submitted for a classification review to a Classified Information Security Officer (“CISO”) designated by the Court. Following the classification review, information deemed unclassified would cease to be treated as classified, while information deemed classified would remain subject to the P.O. In sum, the P.O. would require Defendants to examine the provided discovery materials to decide what is useful or relevant, and request a determination from the CISO (by filing a sealed pleading or otherwise) as to the classified status of particular documents or other information. Only after receiving a decision would Defendants’ pleadings be unsealed in part or in whole, or would Defendants be allowed to publicly disseminate the information in any way. Significantly, information and material that Defendants do not receive from the Government, but glean from public-domain sources or create themselves, would also be subject to the P.O.

Defendants object to the broad coverage of the P.O. and instead ask the Court to require the Government to first perform a classification review of all the material seized from them. The

---

<sup>1</sup>The proposed P.O. denotes this universe of potentially classified information as “Classified Information,” which may have been an unfortunate choice of terms, as it has given rise to accusations that the P.O. changes the statutory definitions of “classified information.” No such change is intended, as discussed in full below. To avoid confusion, the Court will describe the information covered by the proposed P.O. as potentially classified information, which accurately describes its status unless it has already been subjected to a classification review.

Government would be required to designate any of the material that is considered classified information, and only material so designated would be subject to the P.O. In addition, any information Defendants obtained from public-domain sources would be presumed to be unclassified. As discussed below, Defendants' proposal would result in an enormous waste of governmental time and resources, requiring a review of vast amounts of data that Defendants may have no intention of using as part of their defense to the charges they face, and would serve little ascertainable purpose other than to delay this case for an indefinite period of time. Furthermore, contrary to Defendants' many arguments, entry of the proposed P.O. will not cause any violation of Defendants' constitutional rights or principles of fairness. Finally, Defendants' proposal would create a real risk that classified information would be inadvertently disclosed to the public. For the reasons discussed below, the Court has authority to adopt the P.O. proposed by the Government, and will do so with a few modifications.

### **Court's Authority to Enter Protective Order**

This case is subject to the provisions of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. app. 3 §§ 1-16. Many opinions have discussed the purposes and procedures of CIPA generally, and the Court need not repeat that discussion here. *See, e.g., United States v. Lee*, 90 F.Supp.2d 1324, 1325-26 (D. N.M. 2000). For purposes of this opinion, the primary relevant CIPA provision is Section 3, which requires the Court, pursuant to motion by the Government, to enter a protective order preventing disclosure of any classified information "disclosed by the United States to any defendant in any criminal case..." Defendants seize on this phrase and argue that a P.O. issued under CIPA Section 3 only applies fully to information the Government has already determined to be classified and has provided to Defendants in connection with this criminal case. They contend CIPA does not impact information that may or

may not be classified, which they already possessed prior to this case, or to possibly-classified information they may find in the public domain or otherwise develop on their own. It is true that Section 3 of CIPA may not fully cover all the types of information potentially involved in this case, and may not grant the Court authority to require the parties to provisionally treat all the information as classified pending a review by the CISO. *See, e.g., United States v. Pappas*, 94 F.3d 795, 801 (2d Cir. 1996) (CIPA protective order can only prevent disclosure of Defendant's previously-obtained classified information "in connection with trial" and not outside litigation); *cf. United States v. El-Mezain*, 664 F.3d 467, 519-20 (5th Cir. 2011) (CIPA is concerned with court's power to control discovery; implication is CIPA's reach is limited to pendency of a case). However, several other potential sources of power provide ample authority for the Court's action in this case.

First, as in the *Pappas* case, there appear to be enforceable contractual relationships involved here that require protection of classified information, whether or not a certain document has officially been subjected to a classification review. *See* 94 F.3d at 801-02; *see also Snepp v. United States*, 444 U.S. 507, 507-08 (1980) (discussing contractual relationship between CIA employee and government, which survived termination of employment); *United States v. Chalmers*, 2007 WL 591948 (S.D. N.Y. 2007, unpublished) (confidentiality agreement can provide protection against disclosure that CIPA does not). Defense counsel all have been granted security clearances or are in the process of obtaining them, and Defendants themselves formerly possessed such clearances. These clearances include a non-disclosure agreement between the United States and the recipient, obligating the recipient in perpetuity to refrain from disclosing classified information unless such disclosure is authorized. [Doc. 195, Exh. 3] The

non-disclosure agreement applies to all forms of classified information obtained by Defendants or their counsel, not simply information that has already been reviewed by the Government.

In addition, the discovery rules applicable to criminal cases grant the Court broad discretion to enter protective orders of the type proposed here. Fed.R.Crim.P., Rule 16(d)(1) (“At any time the court may, for good cause, ... grant other appropriate relief.”). This rule acts in conjunction with CIPA to allow the Court to control the public dissemination of information provided to or obtained by any party during discovery. *See, e.g., United States v. Aref*, 533 F.3d 72, 78-79 (2d Cir. 2008). It allows the Court to enforce the common-law privilege, held by the Government, against disclosure of state secrets. *See id.*; *see also United States v. Hanjuan Jin*, 791 F.Supp.2d 612, 618 (N.D. Ill. 2011). A court may require that CIPA material be not only theoretically relevant but also actually helpful to the defense, before requiring production. *See United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989). Similar logic prevails here.

The Court also has inherent authority to fill in any holes that might possibly remain after application of CIPA, the rules of discovery, and the common-law privilege regarding state secrets. For example, trial courts have the power, under appropriate circumstances, to preclude parties and counsel from making any extrajudicial statements concerning a pending case, in order to preserve a defendant’s and the public’s right to a fair trial free from prejudicial publicity. *See, e.g., United States v. Tijerina*, 412 F.2d 661, 666 (10th Cir. 1969); *see also Sheppard v. Maxwell*, 384 U.S. 333, 361 (1966) (control of sources of prejudicial news items is “concededly within the court’s power” and the trial court “might well have proscribed extrajudicial statements by any lawyer, party, witness, or court official which divulged prejudicial matters.”); *United States v. Brown*, 218 F.3d 415, 423-24 (5th Cir. 2000) (trial courts have a constitutional duty to minimize the effects of prejudicial pretrial publicity, for the benefit

of both the defendants and the public). Similarly, a trial court certainly has the power to protect the interests of national security by imposing reasonable restrictions on all parties' use of potentially classified information, particularly information related to atomic weapons, in order to prevent harmful dissemination of such information to the public. The public's interest in preserving national security is at least as great as the public's interest in a fair trial. *See United States v. Lee, supra*, 90 F.Supp.2d at 1328 (observing it is obvious that no governmental interest is more compelling than the security of the nation).

### **Information Covered by Protective Order**

According to the Government, there is a mixture of materials in the documents and electronic data seized from Defendants. Some documents are marked "Secret" while others currently await classification review; some of the information apparently is in the public domain already, while other information is not. Defendants contend they produced much of the seized material themselves. As noted above, Defendants maintain the only information that can be subject to the P.O. is information provided by the Government to Defendants, and that is clearly marked as classified. Defendants argue the Government must conduct a classification review of all 276,000 pages of documents and all 5.8 terabytes of electronic information, whether or not the material might be helpful to Defendants, so that Defendants will know what information is classified when they are preparing their pleadings or planning some other type of public dissemination of the information. Defendants point out that CIPA applies only to "classified information" and construe that phrase to mean already-classified information, not information that might be classified but has not yet officially been given that status.

If the Court's authority were limited to that provided by CIPA, it is possible Defendants' argument could be maintained, but as discussed above there are other sources of judicial power

at work here. These other sources afford the Court much broader authority to create and enforce a P.O. than that granted by CIPA alone. The sheer volume of material seized from Defendants militates against adoption of their proposal; requiring advance classification review of all the material would inevitably result in an enormous waste of resources and an indefinite delay in this case. The Court's authority to control discovery as well as its docket, and to prevent any unauthorized communication of classified information, gives the Court the ability to fashion an appropriate remedy to prevent such waste and delay. This appropriate remedy can and does include requiring Defendants to identify documents and other information that might be helpful to their case, and to submit that material to the CISO for a classification review. *Cf., e.g., United States v. El-Mezain*, 664 F.3d 467, 524-25 (5th Cir. 2011) (district court did not err in requiring defendants to request declassification of particular intercepted telephone calls, rather than reviewing tens of thousands of intercepted calls to determine whether they might be helpful to defense; given volume of calls it was not feasible for court to perform the review requested by defendants). It is much more efficient in terms of time, manpower, and money to require Defendants to narrow the amount of material that must be subjected to a classification review, than to require the Government to perform a wholesale review of the mountain of information seized from Defendants. *See id.*; *see also United States v. Poindexter*, 727 F.Supp. 1470, 1480-81 (D.D.C. 1989) (extraordinarily burdensome review of thousands of classified documents not required without a showing of materiality). The Court notes the Government has submitted information indicating that \$3.5 million has already been set aside for classification-review purposes. [Doc. 195, Exh. 4] Furthermore, due to the complexity of classification reviews, it is impossible to predict how long it would take to review all of the material seized from Defendants. [*Id.*] The Court will not add to the expense the Government must incur, or delay

this case indefinitely, by adopting Defendants' proposal requiring a classification review of the material at issue in this case.<sup>2</sup> Instead, the Court will accept the Government's proposal – all discovery provided to Defendants, and any information Defendants may acquire from other sources, will be treated as potentially classified information and covered by the P.O.

The Court will briefly address several other arguments Defendants have raised that are pertinent to this issue. First, Defendants argue that the P.O.'s definition of "Classified Information," which includes all potentially classified information as well as currently classified information, violates the separation-of-powers doctrine. Defendants contend the Court will be changing the definition of "classified information" established by Congress, and found in CIPA, if it adopts this broad definition. This argument is based on a misunderstanding of what the proposed P.O. was intended to do. The P.O. does not change the CIPA definition of "classified information" or change unclassified information to classified, in violation of any statute. Instead, the P.O. simply requires the parties to preliminarily treat all information involved in this case as potentially classified information, and to deal with it in the same manner as actually classified information -- that is, by submitting all pleadings containing any reference to factual information to the CISO for a classification review. If and when it is determined that a pleading

---

<sup>2</sup>The Court has considered Defendants' argument that the Government chose to bring this case, so the burden should be on the Government to determine the classification status of the entire amount of seized material. However, the flip side of this argument is that Defendants engaged in activities that caused a grand jury to indict them. A grand jury has thus found probable cause to believe Defendants had possession of classified information and either attempted to or did misuse that information. See *United States v. Windrix*, 405 F.3d 1146, 1153 (10th Cir.2005) (grand-jury indictment provided probable cause to believe that defendants were involved in crime). It is therefore appropriate to put the burden on Defendants, who presumably are familiar with the documents and electronic data seized by the Government, to narrow the scope of the required classification review by initially identifying those materials that will be helpful to them, which can then be reviewed for classification status.

contains no classified information, it will be unsealed and any documents, electronic data, or other information referenced in the pleading may thenceforth be handled as unclassified information.<sup>3</sup> No violation of the separation-of-powers doctrine will have occurred.

Defendants also point out that a (perhaps substantial) portion of the seized material is already in the public domain, and that they may wish to use other public-domain information in their pleadings. They argue they should not have to guess what public-domain information is classified and what is not, in preparing their pleadings. The short answer is, there is no need to guess – the P.O. applies to all factual information Defendants may wish to submit to the Court or otherwise disseminate publicly, including public-domain information. All Defendants have to do is submit any factual information or materials of any kind to the CISO, who will promptly have a classification review performed. This will eliminate any guesswork on Defendants’ part. The Court notes it is well-accepted that the mere fact that information may appear in the public domain does not mean it is not classified. *See, e.g., Fitzgibbon v. C.I.A.*, 911 F.2d 755, 765-66 (D.C. Cir. 1990) ; *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir.1975). Thus, public-domain information must be handled in the same manner as any other information Defendants may wish to disseminate or submit to the Court.

As a final note, the Court points out that material that is created by a defendant may also constitute classified information. *See, e.g., United States v. Poindexter, supra*, 698 F.Supp. at 320 (discussing difficulties posed by unusual case in which defendant had authored or already received much of the classified information involved in the case). Defendants’ claim that they

---

<sup>3</sup>As the Court noted above, it may be unfortunate that the proposed P.O. uses the term “Classified Information” to refer not just to classified information as defined by statute, but also to potentially classified information, as this has apparently caused some confusion. Reading the P.O. in conjunction with this opinion, however, should prevent any further confusion.

produced much of the material seized by the Government will not change the manner in which the material must be handled.

**Procedural Requirement – Submission of Material to CISO for Classification Review**

Defendants have raised several objections to the process created by the P.O., under which all factual submissions to the Court, or other public disseminations of factual information, must be submitted to the CISO for classification review prior to such submission or dissemination. Specifically, any pleading submitted for filing must be filed under seal and submitted to the CISO. The CISO will then obtain a classification review from the appropriate agency; if no classified information is involved the pleading will be unsealed in its entirety. This requirement will not apply to purely ministerial pleadings, such as requests for extensions of time or page limits, but will be applicable to any pleading containing substantive argument or information. Similarly, any other material Defendants may contemplate using at trial or otherwise disseminating publicly must be first submitted to the CISO for classification review.

Defendants' first objection to the process contemplated by the P.O. is that there is no reason to submit every pleading to the CISO under seal; the only pleadings that should be subjected to such treatment are those containing classified information, which Defendants define narrowly to mean only material that has already been subjected to a classification review and determined to be classified. The Court has already rejected Defendants' attempt to force the Government to review for classified status the entire body of material that will be provided in discovery. Therefore, to prevent classified information from being inadvertently disclosed, it is necessary to require the parties to submit every substantive pleading to the CISO under seal, so a classification review can be performed at the time of filing. This burden should generally be small; the Court notes the Government's reply brief with respect to this motion was filed under

seal and submitted to the CISO, and only a few days passed before a classification review was performed and the entire pleading unsealed.

Defendants also contend their First Amendment rights and their right to an open trial will be violated if they are required to file all pleadings under seal. The Court notes that First Amendment rights, as well as the right to an open trial, are not absolute. *See United States v. Brown, supra*, 218 F.3d at 424-25. Instead, these rights may be subjected to reasonable limitations that are narrowly tailored to protect a significant competing interest, such as the right to a fair trial. *See id.* Defendants must certainly concede that national security is such a compelling interest, and that they have no constitutional right to disseminate classified information publicly. The requirement that pleadings be first filed under seal does not permanently conceal unclassified information, as Defendants seem to contend. Once the classification review is performed, unclassified portions of the pleadings will be unsealed and open to the public. The minimal delay caused by this procedure constitutes only a slight burden on the First Amendment as well as on Defendants' right to an open trial, and has the salutary effect of ensuring that only unclassified information is available for public review. *See United States v. Rosen*, 520 F.Supp.2d 786, 797 (E.D. Va. 2007) (CIPA redactions do not effect a closure of the trial to the public; same information available to parties is available to public); *United States v. Ressam*, 221 F.Supp.2d 1252, 1263-64 (W.D. Wash. 2002) (redaction of classified information was narrowly tailored to protect governmental interest in security, and did not violate First Amendment).

Defendants also contend their right to remain silent will be violated if they are required to submit to the CISO, for classification review, all documents or other material they may plan to use at trial. They contend that doing so will require them to reveal the content of any testimony

they may contemplate giving at the trial, which will impermissibly burden their right to remain silent. Defendants recognize this argument has been rejected by many courts, including a judge in this very district. *See United States v. Lee, supra*, 90 F.2d at 1327. However, Defendants attempt to distinguish this case from *Lee* and others by pointing out that the disclosure requirement in this case will be much broader, as it will apply not only to actually classified information but also to all of the potentially classified information involved here. This argument lacks merit for two reasons. First, if disclosure of a certain amount of information does not burden a defendant's right to remain silent, it is difficult to understand why disclosure of a greater amount of information would do so. Second, and more significantly, Defendants' argument equates submission of information to the CISO with disclosure of that information to the Government. This will not be the case. The CISO is a neutral party and will have no communication with the prosecution team. Furthermore, by this opinion the prosecution team is instructed to have no communication with the individuals performing the classification reviews requested by the CISO, as to any requests for review that might have been submitted by Defendants. Thus, Defendants can have no concern that the Government will become aware of any testimony Defendants might be thinking of giving.

Defendants raise a quite similar argument by contending their rights to due process and effective representation by counsel will be violated if they are forced to reveal their thought processes to the Government prior to trial. They maintain this will happen if they are required to submit all material they might plan to use at trial to the CISO for pre-use classification review. Again, the short answer to this contention is that submission to the CISO is not the equivalent of submission to the Government; the Government should in no way become aware of what material Defendants have submitted to the CISO for review. In sum, the CISO-submission

process will not require Defendants to reveal anything more to the Government than an “ordinary” CIPA case would. Defendants must simply undergo an extra step here, by obtaining CISO review of any information they plan to use at trial; only if the information is determined to be classified will they need to disclose the planned use pursuant to Section 5 of CIPA. It should be noted that the pretrial notification requirements of CIPA do not in any way violate due process. *See United States v. Hashmi*, 621 F.Supp.2d 76, 81 (S.D. N.Y. 2008); *United States v. North*, 708 F.Supp. 399, 401 (D.D.C. 1988) (due process is even-handed concept; defendant cannot accept discovery and then expect to avoid disclosing information of his own).

Defendants also argue the P.O. is overbroad and vague, and they should not have to guess which pleadings might contain classified information and thus should be sealed, or what material that might be useful for trial contains classified information. Accordingly, they repeat their contention that the Government should be required to perform a classification review on all the material in its possession before Defendants begin to use the material. Again, the answer to this contention is easy. Defendants do not need to guess about the classified nature of anything; they simply must submit anything they might want to disclose, in pleadings or at trial or otherwise, to the CISO for a review which will definitively settle the issue of whether or not any classified information is implicated. No guesswork will be involved at any point.

### **Creating A Negligence Standard for Criminal Liability**

Defendants complain that the P.O. impermissibly creates a negligence standard for criminal or contempt liability, in contravention of settled principles of law. They point to a provision in the P.O. cautioning against unauthorized disclosures of classified information, which states as follows: “Any negligent handling or unauthorized disclosure or retention of Classified Information could cause serious damage – and possibly exceptionally grave damage –

to the national security of the United States, may be used to the advantage of a foreign nation against the interests of the United States, and **may** constitute a violation of United States criminal laws.” (emphasis added). The provision adds that violations of the P.O. “**may** result in a charge of contempt of court and possible referral for criminal prosecution.” (emphasis added). [Doc. 171, Exh. 1, proposed P.O. § 15] According to Defendants, this provision creates a negligence standard that will then be used to impose criminal charges or contempt-of-court citations. The provision does no such thing. It is merely a cautionary admonition, rightly pointing out the harm that could result from either deliberate or negligent unauthorized disclosure of classified information, and indicating possible consequences for the individual that **may** be imposed by the Court for such actions. The provision will of course be construed and applied consistently with criminal statutes and the law of criminal or civil contempt. If under those authorities negligent acts cannot lead to criminal liability or contempt, the possible consequences recited in the provision will not come to pass. The Court does note, however, as did the Government, that at least one statute applicable to a type of classified information criminalizes gross negligence in the handling of such information. 18 U.S.C. § 793(f). The premise underlying Defendants’ argument may therefore be itself questionable.

### **Right to Challenge Classification Decisions**

Defendants have proposed an addition to the P.O. detailing their alleged right to challenge classification decisions made by the CISO or the individuals consulted by the CISO. Defendants cite to federal regulations concerning classification decisions, and request that the Court create a system that would include a hearing for each challenged classification decision, under which the Court would decide whether the individuals making the classification decisions had complied with the applicable regulations. According to Defendants, they are entitled to such

hearings because the classification regulations create a property interest enforceable under the due-process clause. Defendants have cited no case supporting their assertion that they are entitled to challenge classification decisions made by representatives of particular federal agencies.

The Government, on the other hand, contends classification decisions are executive in nature rather than judicial, and may not be challenged in court. Support for that proposition may be found in several cases, mostly from the Fourth Circuit, although discussion of the question is not extensive in any of them. *See, e.g., United States v. Abu Ali*, 528 F.3d 210, 253 (4th Cir. 2008) (“We are not asked, and we have no authority, to consider judgments made by the Attorney General concerning the extent to which the information in issue here implicates national security.”); *United States v. Collins*, 720 F.2d 1195, 1198, n. 2 (11th Cir. 1983); *United States v. Musa*, 833 F.Supp. 752, 755 (E.D.Mo. 1993). At least one Circuit has declined to address the question. *United States v. Aref*, 533 F.3d 72, 82 (2d Cir. 2008). Other Circuits indicate courts do have the power, in the context of requests submitted under the Freedom of Information Act, to review classification decisions of agencies such as the CIA. *See McGehee v. Casey*, 718 F.2d 1137, 1148-49 (D.C. Cir. 1983); *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1367 (4th Cir. 1975).

This appears to be a potentially complicated issue that Defendants would have the Court decide in the abstract, with no explanation of why a particular classification decision might impair their defense or otherwise affect this case in any way. The Court declines to adopt Defendants’ proposal, as it would create a real risk that this case will devolve into an endless series of hearings concerning the propriety of classification decisions made by the CISO. Should there be a genuine, significant reason, related to the defense of this case, that Defendants wish to

challenge a specific classification decision as to a specific piece of information, Defendants may raise this issue again in that narrow context. Defendants should locate persuasive authority requiring the Court to consider such a challenge, and the Court will still determine whether a challenge might be appropriate. The Court will take into account the need to keep this case moving and avoid unproductive forays into collateral matters, as well as the need demonstrated by Defendants to challenge that particular classification decision. *See United States v. Passaro*, 577 F.3d 207, 219 (4th Cir. 2009) (CIPA provides framework under which court can balance defendant's interest in a fair trial and the Government's interest in protecting national security information); *see also United States v. Stewart*, 590 F.3d 93, 131 (2d Cir. 2009) (to be disclosable under CIPA, classified information must be relevant and helpful or material to the defense). At this time, however, as noted above, the Court finds no basis to create the hearing process requested by Defendants that would allow wholesale challenges to any and all classification decisions made by the CISO.

#### **Duration of Protective Order**

Defendants contend the P.O. should remain in effect only for the duration of this litigation. The Government, on the other hand, argues that classified information must be protected in perpetuity, at least until it is declassified. The Court's authority to control the handling and dissemination of information while this case is pending is unquestionable. However, CIPA was designed only to authorize a court's order restricting the dissemination of material in connection with court proceedings. *See United States v. Pappas*, 94 F.3d 795, 800-801 (2d Cir. 1996). Similarly, the other sources of authority for the Court's issuance of a P.O. arise primarily from the Court's control over discovery matters and the docket, as well as the inherent authority to issue orders to litigants appearing before the Court. Thus, the power over

the parties derived by the Court from CIPA and from the litigation-related sources of authority arise due to the Court's control over this litigation and are designed to control the parties' actions during the litigation; it would seem logical that this power will expire at the termination of the case. *Cf. United States v. Harris*, 582 F.3d 512, 515-16 (3d Cir. 2009) (where civil contempt order is coercive in nature, and thus intended to influence conduct during pendency of litigation, it becomes moot when litigation is terminated); *United States v. Kane*, 625 F.3d 568, 573-74 (9th Cir. 2010) (trial subpoena expires when criminal case is terminated by plea).

As for the apparent contractual relationship between the parties, it is true that an agreement requiring non-disclosure of classified information in perpetuity would seem to allow the Government to bring an action to enforce the terms of that contract if a breach appears imminent. What the Government is asking for at this point, however, is an order that has the effect of a do-not-breach-the-contract injunction that is not limited to the handling and dissemination of classified information, but also applies to potentially classified information. This latter category of information, depending on the results of a classification review (should one be performed) may or may not be subject to the non-disclosure contract between the parties, as that agreement appears to preclude disclosure only of classified information.<sup>4</sup> Furthermore, there has been no showing that a breach of the non-disclosure agreement is imminent, or that Defendants will even be in a position to breach the agreement following the conclusion of this criminal case. *See, e.g., Holiday Inns of America, Inc. v. B & B Corporation*, 409 F.2d 614, 618

---

<sup>4</sup>The Court also notes the First Amendment may be implicated to the extent the Government, through the P.O., might seek to control use and dissemination of unclassified information, following the close of this litigation. *See, e.g., United States v. Marchetti*, 466 F.2d 1309, 1317 (4th Cir. 1972) (due to First Amendment concerns, circuit court "would decline enforcement of the [employment-related] secrecy oath ... to the extent that it purports to prevent disclosure of unclassified information...").

(3d Cir. 1969) (injunction “may not be used simply to eliminate a possibility of a remote future injury, or a future invasion of rights, be those rights protected by statute or by the common law.”). The Government’s request for a permanent P.O. appears to be premature at this time.

In sum, it appears the Government’s post-litigation remedies will more properly be afforded by contract law or by the criminal laws proscribing public dissemination of classified information, rather than a permanent P.O. issued in this case. In the absence of convincing authority to the contrary, it is sufficient that the P.O. is in effect while the case is pending. Any remaining questions concerning protection of classified information following the termination of this criminal case may be addressed in an appropriate proceeding at the appropriate time.

### **Ownership of Seized Material**


The proposed P.O. includes a provision stating that “All Classified Information to which the Defense has access in this case is now and will remain the property of the United States.” [Doc. 171, Exh. 1, § 16 of proposed P.O.] Defendants object strongly to this provision, arguing that they remain the owners of the seized material, at least to the extent it consists of unclassified information. Defendants maintain that if the Government wants to obtain ownership of their property it must initiate a forfeiture proceeding. The Government did not respond to this argument in the reply brief. The Court notes that the Government’s claim of ownership in the proposed P.O. is not limited to actually classified information, but applies to “Classified Information,” which includes all potentially classified information seized from Defendants, even if that material may eventually be determined to be unclassified. It is not clear to the Court why the Government should be entitled to permanent ownership of unclassified information seized from Defendants. It is also not clear to the Court what, if anything, this provision adds to the P.O. It seems to the Court that litigation over ownership of the unclassified information

involved in this case is a collateral matter that need not be decided in the context of this motion. Should there be a need to decide ownership issues at this time, which frankly the Court does not think likely, the Government may file a separate motion addressing that question. For now, the Court will not delay issuance of the P.O. and the commencement of discovery so this question can be litigated. The Government is instructed to remove the “ownership” language contained in Section 16 of the proposed P.O. from the revised version the Government must submit for the Court’s signature.

### **Conclusion**

As discussed above, the Court will adopt the proposed P.O. submitted by the Government, with the following provisos: (1) the “ownership” language found in Section 16 must be removed; (2) the term “Classified Information” is understood to mean potentially classified information, rather than information that has been determined to be classified; and (3) any language in the P.O. addressing the duration of the P.O. should make it clear the P.O. remains in effect for the duration of this case. The Government should submit a revised version of the P.O. for the Court’s signature as soon as is practicable.

Dated this 9<sup>th</sup> day of February, 2012.

 \_\_\_\_\_  
BRUCE D. BLACK  
United States District Judge